

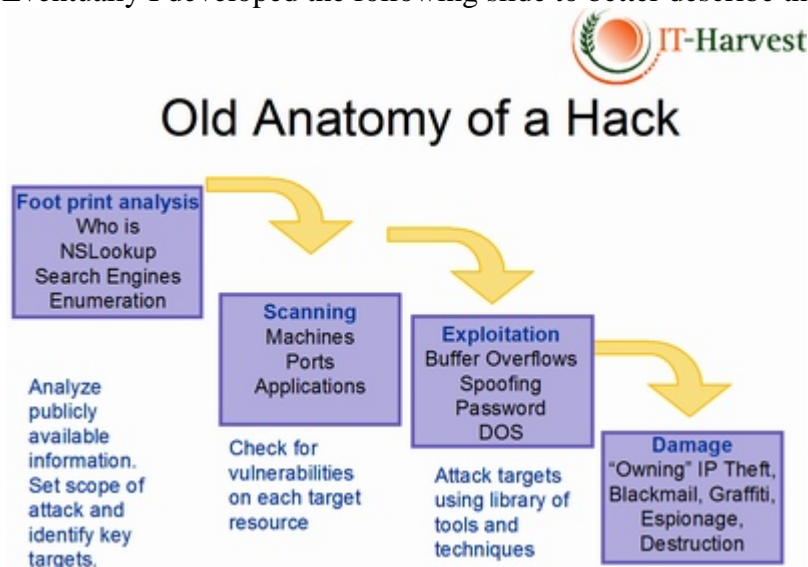


Best of ThreatChaos

## [New anatomy of a hack](#)

As a white-hat hacker for a big audit firm I spent days and nights in our “lab” launching scans and scripted attacks against client networks. Other than the possession of a “get-out-of-jail-free card”, a signed agreement from the customer, our methodologies were the same as any hacker’s.

Eventually I developed the following slide to better describe the anatomy of a hack.

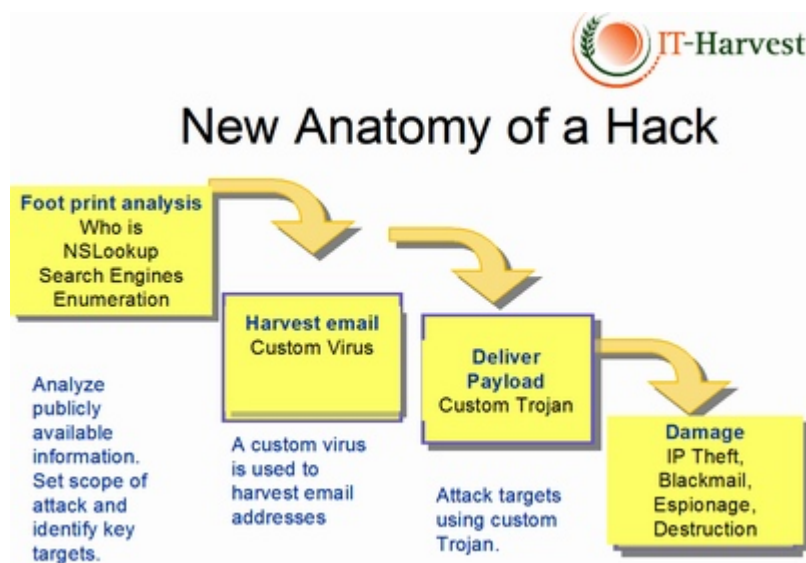


The most interesting stage of a targeted attack is the reconnaissance, or footprint analysis. Here you use the web, search engines, whois, and [nslookup](#), to discover as much about the target as possible. A whois lookup can tell you email address formats for instance (first letter last name @ company.com). An improperly configured DNS server could reveal machine names to an nslookup query (payments.company.com). A Google search could reveal submission to forums by security personnel that reveal brands of firewall or antivirus in use at the target. Sometimes network diagrams are even found that can guide an attack. The next stage, scanning, meant using special tools, ( I date myself by mentioning Cybercop and Internet Security Scanner, these were the days before the open source [Nessus](#)) to discover open ports, services, and machines on the

target network. And then, finally, you could start attacking various vulnerabilities that you had discovered.

This cook-book methodology is still the same used by attackers and security consultants that are hired to test your preparedness. However, as I looked at that slide in preparation for a seminar I am giving on the security market, I realized that it needs to be updated to account for recent developments: in particular, the use of Trojans to slip inside a network and steal information directly.

The new anatomy of a hack looks like this picture.

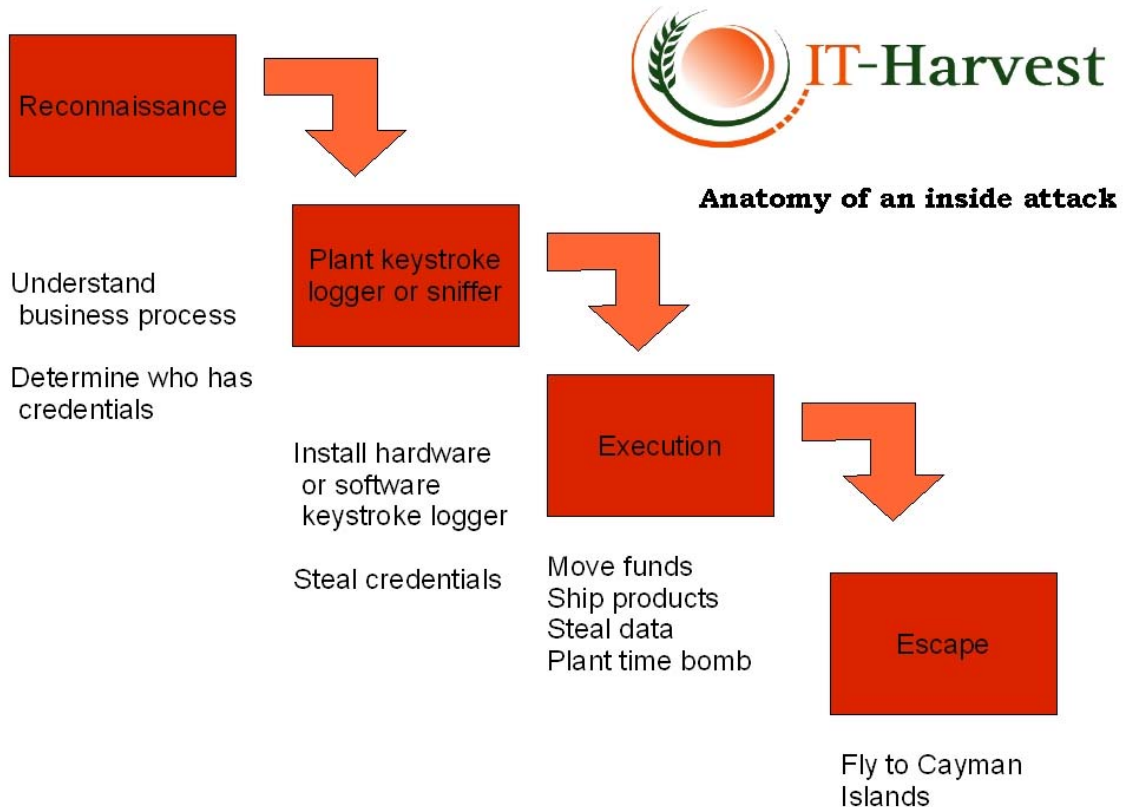


The attacker still needs to know their target, and thus the footprint analysis, but then they proceed to use custom viruses and Trojans to infiltrate the target. The Trojans then harvest files, email, and keystrokes and send them back to home base. What is chilling is that this is so much easier than the old methodology. And, according to the National High Tech Crime Unit in the UK(now [SOCA](#)), it is being used against UK businesses and government agencies on an industrial scale.

And Now: The Anatomy of an Insider Attack

While the techniques of hackers from the outside are fascinating, the methods used by insiders are worth looking at too. It is harder to create a simple anatomy of an inside hack because they take so many forms. Look at the now most infamous insider attack. Jerome Kerviel spent hours in the evening “hacking” into Societe Generals’s computer systems. He eliminated trading controls put in place to impose limits on the size of bets he could make. He logged in using the credentials of his friends in the back office where he used to work. The end result was over \$7

billion in losses. I have to draw on my PwC experience to create a picture of the insider approach.



While an auditor must quickly assess controls and find holes an insider has much more time to determine where an organization may have a weak link. That weak link usually takes the form of too much trust extended to particular people. If a sys admin at a major railroad has access to the software that routes trains for instance, he may figure out which car of valuable electronic equipment to shunt to a siding where his accomplices can loot it. A trader or banker may notice that there is an untraceable way to transfer funds to a personal account. The first step of insider attack is recognizing an “opportunity”. It might involve figuring out who has access to the systems needed to execute a theft.

The second step is to acquire the credentials of a privileged user. This can be done with a simple hardware keystroke logger or even by loading a Trojan Horse on the target’s computer. If there are tokens involved it might involve stealing those first.

The “execution” phase is when the insider pulls off his attack. He transfers the money, ships the product to his home, downloads the data to a thumb drive, or performs a trade that will profit him.

The final phase is “escape”. We will never know about the many insiders that escape. Even if they are detected most organizations do not report successful insider attacks. Luckily there are some that are apprehended and prosecuted. Pay attention to those cases as they could reveal weaknesses in your own organization.